W. DOUGLAS SPRAGUE (Bar No. 202121)
COVINGTON & BURLING LLP
Salesforce Tower
415 Mission Street, Suite 5400
San Francisco, California 94105-2533
Telephone: (415) 591-6000
Facsimile: (415) 591-6091
Email: dsprague@cov.com

MEGAN A. CROWLEY (*pro hac vice* pending)
CHLOE GOODWIN (*pro hac vice* pending)
COVINGTON & BURLING LLP
One City Center
850 Tenth Street, NW
Washington, DC 20001-4956
Telephone: (202) 662-5367
Facsimile: (202) 662-6291
Email: mcrowley@cov.com
cgoodwin@cov.com

Attorneys for Third Party Microsoft Corporation

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, *Plaintiff* v. CIAN BURLEY *Defendant*.	No. 21-CR-00198 EMC **DECLARATION OF MEGAN A. CROWLEY**

I, MEGAN A. CROWLEY, hereby declare:

1. I am a partner at the law firm of Covington & Burling LLP, counsel for Microsoft Corporation ("Microsoft"), and am fully familiar with the facts, circumstances, and proceedings herein.

2. On March 6, 2023, I conferred with Defendant's counsel about the Rule 17(c) subpoena that Defendant served on Microsoft. During that call, I explained that Microsoft objected to the majority of Defendant's requests because they fail Rule 17's specificity, relevance, and admissibility requirements. I also explained that Microsoft does not have records identifying the individual who conducted the manual review of the images at issue in this case, nor the time or place of such review, out of concern for the privacy and safety of the individuals engaged in this work. I offered to point Defendant to publicly available information responsive to many of his requests, including materials on Microsoft's website and employee declarations filed in other cases involving PhotoDNA. Defendant's counsel agreed to hold open Microsoft's deadline for responding to the subpoena while the parties continued to negotiate.

3. On March 20, 2023, I again conferred with Defendant's counsel about Defendant's subpoena. During that conversation, I agreed to provide further public information to resolve Request 2, along with a declaration from a Microsoft employee containing information to resolve Requests 4 and 6, and part of Request 10. (By this time, the parties had resolved Requests 1, 3, 7, 8, 9, and 11 via e-mail.) However, the parties were unable to come to an agreement on Request 5 and the remainder of Request 10.

4. During the March 20, 2023 call, I explained that Request 5 and the disputed portion of Request 10 exceed the scope of Rule 17 because any responsive materials would be neither relevant to nor admissible at a suppression hearing, and because Defendant did not describe the records sought with specificity. Defendant's counsel asserted, in turn, that the materials were relevant because they would shed light on Microsoft's procedures for reviewing suspected child pornography in the normal course, such as who typically conducts reviews, what the review consists of, and when the review takes place. Defendant's counsel stated this information may support Defendant's motion to suppress, in which he will argue that the government's warrantless review of the four images submitted to NCMEC does not fall within the "private search" exception to the Fourth Amendment.

5. The parties conferred for the final time on March 31, 2023. I asked again why Defendant thought the materials sought by Requests 5 and 10 were relevant, and reiterated why, in Microsoft's view, they were not. I also asked Defendant to confirm that the reason he requested these materials is because he hoped they would reveal how Microsoft conducts review of suspected child sexual exploitation and abuse imagery in the regular course. Defendant's counsel confirmed that this was an accurate statement of Defendant's position. In an effort to resolve this issue without court intervention, I asked whether there was a way to resolve this issue through a declaration, and suggested that Microsoft could include language in its declaration providing an overview of its process for confirming that a hash match flagged by PhotoDNA is child sexual exploitation and abuse imagery, thereby providing the information Defendant seeks through Requests 5 and 10. Defendant's counsel rejected that offer. At that point, we agreed we were at an impasse, and Microsoft would file a motion to quash Request 5 in its entirety and Request 10 in part.

6. Attached as **Exhibit A** is a true and correct copy of Defendant's Rule 17(c) subpoena, served on Microsoft on February 23, 2023.

7. Attached as **Exhibit B** is a true and correct copy of Microsoft and Defendant's e-mail correspondence between March 14, 2023, and March 29, 2023.

8. Attached as **Exhibit C** is a true and correct copy of CyberTipline Report 52016239.

9. Attached as **Exhibit D** is a true and correct copy of Microsoft and Defendant's e-mail correspondence between March 2, 2023, and March 8, 2023.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge. This declaration was executed on April 10, 2023, in Washington, D.C.

/s/ Megan A. Crowley
Megan A. Crowley

Exhibit A

CAND 89B (Rev. 8/12) Subpoena to Produce Documents or Objects in a Criminal Case

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

CIAN BURLEY

Defendant(s).

SUBPOENA TO PRODUCE DOCUMENTS OR OBJECTS IN A CRIMINAL CASE

Case No.: 21-cr-00198 EMC

TO: Custodian of Records
Microsoft Corporation

YOU ARE COMMANDED to produce at the place, date, and time specified the document(s) or object(s) indicated below. If compliance would be unreasonable or oppressive, you may file a motion requesting the court to quash or modify the subpoena, to review the documents in camera, or to permit production only pursuant to a protective order.

PLACE

☑ United States Courthouse
450 Golden Gate Avenue
San Francisco, CA 94102

☐ United States Courthouse
280 South First Street
San Jose, CA 95113

☐ United States Courthouse
1301 Clay Street
Oakland, CA 94612

COURTROOM/JUDGE
Hon. Edward M. Chen
Floor 17, Courtroom 5

DATE AND TIME
03/08/2023
2:30 PM

If the document(s) or object(s) are produced in advance of the date specified, either to the court in an envelope delivered to the clerk's office or to the issuing attorney whose name and address appears below, no appearance is necessary.

The following document(s) or object(s) shall be produced:

See Attachment A.
*DELIVERY OF CERTIFIED AND UNREDACTED COPIES OF ALL RESPONSIVE RECORDS TO THIS COURT, OR TO ONE OF THE REPRESENTATIVES OF THE FEDERAL PUBLIC DEFENDER'S OFFICE LISTED BELOW, PRIOR TO THE APPEARANCE DATE MAY SUFFICE IN LIEU OF PERSONAL APPEARANCE.

NOTE: Subpoena forms requiring the appearance of a witness to testify at a criminal proceeding or to testify and bring documents to a criminal proceeding, must use Form CAND 89A, *Subpoena to Testify in a Criminal Case*) or for the production of state law enforcement personnel or complaint records (CAND 89C, *Subpoena to Produce State Law Enforcement Personnel Or Complaint Records in a Criminal Case*) are available at the Court's Internet site: cand.uscourts.gov.

U.S. MAGISTRATE JUDGE OR CLERK OF COURT

Mark Busby

(By) Deputy Clerk

Vicky L. Ayala

DATE February 15, 2023

ATTORNEY'S NAME, ADDRESS AND PHONE NUMBER:

JODI LINKER, Federal Public Defender
GABRIELA BISCHOF, Assistant Federal Public Defender
450 Golden Gate Ave., Box 36106
San Francisco, CA 94102
Rob Ultan, Investigator (415) 436-7700 email: robert_ultan@fd.org

PROOF OF SERVICE		
RECEIVED BY SERVER	DATE	PLACE
SERVED	DATE	PLACE
SERVED ON (PRINT NAME)		FEES AND MILEAGE TENDERED TO WITNESS ☐ YES ☐ NO AMOUNT $
SERVED BY (PRINT NAME)		TITLE

DECLARATION OF SERVER

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Proof of Service is true and correct.

Executed on _____ _____

DATE SIGNATURE OF SERVER

ADDRESS:

ADDITIONAL INFORMATION

ATTACHMENT A to Microsoft Subpoena

United States v. Cian Burley, CR 21-00198-EMC

All records responsive to any of the following:

1. All materials, including reports, emails, documents, or other written and unwritten materials, related to the CyberTip report (CT # 56016239) submitted by Microsoft[1] to NCMEC and law enforcement agencies including the entire contents of that report.

2. A detailed description of the method(s) by which image files were located by Microsoft, including but not limited to the manner in which hash values are assigned to the original photographs and the images deemed to replicate them and any validation studies or other information regarding the reliability of Microsoft's programs in identifying such original images and images deemed to replicate them.

3. Any documentation and description related to CyberTip # 56016239 of all actions Microsoft undertook in relation to the images and/or associated Skype chats or file storage, before reporting them to NCMEC, including but not limited to whether an employee at Microsoft reviewed one or more of the four images contained in the CyberTip Report, the identity of the Microsoft employee(s) who viewed the images, which image they each viewed, when they viewed the images, the identity of the employee who submitted the report and files to NCMEC and when, and all records, in any form, that memorialize any and all of these actions.

4. Any records and information, in any form, pertaining to whether Microsoft has used an automated system, not requiring a Microsoft employee, to generate and submit CyberTip reports with NCMEC, including the dates when such an automated system was in effect. If Microsoft used such an automated system at the time of the CyberTip referenced above, please provide a detailed description of the system etc.

5. Any training materials used to train Microsoft employees on the definitions of child pornography, company reporting procedures for located suspected child pornography, classification standards of suspected child pornography.

6. Any reports, emails, documents or other written and unwritten materials describing or related to any automated reporting system used at any time by Microsoft to report suspected child pornography to NCMEC and/or police agencies. If Microsoft does not possess any of these materials, information as to whether Microsoft ever used an automated reporting system and when.

7. All correspondence, in any form, to NCMEC, Microsoft, or law enforcement agencies from Microsoft's PhotoDNA program, or the API associated with the PhotoDNA program, related to the CyberTip report referenced above.

---

[1] As used herein, Microsoft refers to Microsoft Corporation, as well as its parents and subsidiaries, including but not limited to Microsoft Online Services, Skype, and any subsidiaries related to its PhotoDNA technology.

8. All materials, including reports, emails, documents, or other written and unwritten materials in Microsoft's possession, custody or control related to NCMEC's response to the CyberTip report identified above, including all actions taken by NCMEC with respect to any information received from Microsoft, such as opening any emails, opening any attachments, conducting any investigation, and forwarding any information to law enforcement.

9. Any and all policies and procedures, reports, guidelines, manuals, operating agreements, letters of understanding, memoranda, meeting notes or other materials, regarding Microsoft's reporting to, and relationship with NCMEC, the federal Department of Justice including the the Federal Bureau of Investigation, the Santa Rosa Police Department, the Sonoma County Sheriff's Office, or any other state and local law enforcement, including but not limited to:

    a. All correspondence between NCMEC and Microsoft concerning requests NCMEC made to Microsoft to sign up for its CyberTip line.

    b. Documents sufficient to show any request NCMEC sent to or received from Microsoft concerning Microsoft's PhotoDNA program addressing the financing or technical development of the PhotoDNA software or any associated API, or NCMEC's specific needs or software requirements to run the program or any associated API.

    c. All registration materials related to the registration of Microsoft or Microsoft's subsidiary PhotoDNA for NCMEC's CyberTip line.

    d. All of NCMEC's Memoranda of Understanding or similar agreements with Microsoft addressing the sharing of NCMEC's library or platform of hash values associated with contraband.

    e. Any communications between Microsoft and any law enforcement agency concerning Microsoft's investigation into Cian Burley or CyberTip # 56016239.

10. Any and all policies, procedures, reports, guidelines, manuals, or other materials, regarding the discovery, review, and/or reporting of accounts for suspected child pornography by Microsoft, whether manual or automated; a description of any technology or methods used to search user data, including PhotoDNA and/or similar technologies or methods; and, any communications with employees regarding user/subscriber content to be flagged.

11. Microsoft's Privacy Policy and Terms of Service in effect from July 30, 2018, to January 13, 2020.

Exhibit B

From: Crowley, Megan
Sent: Wednesday, March 29, 2023 8:40 PM
To: Karthik Raju; Gabriela Bischof
Cc: Goodwin, Chloe; Robert Ultan
Subject: RE: United States v. Burley, No. 21-CR-00198 EMC

Yes, Friday works. We will circulate a link for a call at 1:30 PT/4:30 ET.

Thanks,
Megan

From: Karthik Raju <Karthik_Raju@fd.org>
Sent: Wednesday, March 29, 2023 6:40 PM
To: Crowley, Megan <MCrowley@cov.com>; Gabriela Bischof <Gabriela_Bischof@fd.org>
Cc: Goodwin, Chloe <CGoodwin@cov.com>; Robert Ultan <Robert_Ultan@fd.org>
Subject: RE: United States v. Burley, No. 21-CR-00198 EMC

[EXTERNAL]
Hi Megan,

Unfortunately, this evening doesn't work and tomorrow is filled with court appearances.

Are you available for a conversation on Friday afternoon after 1pm PST?

Thanks,
Karthik

From: Crowley, Megan <MCrowley@cov.com>
Sent: Wednesday, March 29, 2023 2:05 PM
To: Gabriela Bischof <Gabriela_Bischof@fd.org>; Karthik Raju <Karthik_Raju@fd.org>
Cc: Goodwin, Chloe <CGoodwin@cov.com>; Robert Ultan <Robert_Ultan@fd.org>
Subject: RE: United States v. Burley, No. 21-CR-00198 EMC

EXTERNAL SENDER
Hi Gabriela,

Thanks for your reply. We do not view these modifications to bring your requests within the scope of Rule 17, for the reasons set out in my prior e-mail, but think it would be useful to discuss. There also appears to have been a miscommunication on our last call -- where Microsoft has agreed to conduct a reasonable search for records responsive to your requests, it will make a production of responsive documents and I will confirm that no other responsive documents were located, as is customary for a subpoena response.

Are you available for a call today sometime between 5:30 and 7:30 pm PT, or tomorrow between 11 am and 2 pm PT?

Thanks,
Megan

From: Gabriela Bischof <Gabriela_Bischof@fd.org>
Sent: Monday, March 27, 2023 4:26 PM

To: Crowley, Megan <MCrowley@cov.com>; Karthik Raju <Karthik_Raju@fd.org>
Cc: Goodwin, Chloe <CGoodwin@cov.com>; Fitch, James <JHFitch@cov.com>; Robert Ultan <Robert_Ultan@fd.org>
Subject: Re: United States v. Burley, No. 21-CR-00198 EMC

[EXTERNAL]

Hi Megan,

Thanks for sending your email below. We've reviewed it carefully and modified our requests (5) and (10) to the following:

5. The training materials used to train Microsoft employees on the definitions of child pornography, company reporting procedures for located suspected child pornography files, and classification standards of suspected child pornography in effect around the time of CyberTip 52016239, from July 5, 2019, [suspected CP first flagged] until August 7, 2019 [date when NCMEC processed the CyberTip].

10. The policies, reports, guidelines, and manuals that set forth the procedures for review, and reporting of accounts containing suspected child pornography files, whether manual or automated; a description of any technology or methods used to search those flagged accounts; and, any communications with employees regarding user/subscriber content to be flagged related to CyberTip 52016239 or user live:ciank111980, from July 5, 2019, [suspected CP first scanned] until August 7, 2019 [NCMEC date processed].

I also wanted to memorialize our understanding that where Microsoft conducts a reasonable search and no information related to a particular requested item is found, the fact of that search and the lack of records will be included in the declarations submitted in response to the subpoena.

I hope this resolves your concerns. If not, I think it may be time to bring our remaining issues to Judge Chen. I am happy to talk more if you think that would be fruitful, and can be reached at 415-517-2593.

Best,
Gabriela

From: Crowley, Megan <MCrowley@cov.com>
Sent: Wednesday, March 22, 2023 2:48 PM
To: Gabriela Bischof; Karthik Raju
Cc: Goodwin, Chloe; Fitch, James; Robert Ultan
Subject: RE: United States v. Burley, No. 21-CR-00198 EMC

EXTERNAL SENDER

Hi Gabriela,

Thank you for the call on Monday. As discussed, we plan on drafting a declaration for this case, which will include a description of PhotoDNA and how it works, along with the additional information we discussed, to resolve requests 4, 6, and 10 (in part). We are also directing you to Dr. Farid's Congressional testimony here, to resolve request 2.

We are writing now to set out our position on why request 5 and the unresolved portion of request 10 go beyond the scope of Rule 17. These requests seek "[a]ny training materials used to train Microsoft employees on the definitions of child pornography, company reporting procedures for located suspected child pornography, classification standards of suspected child pornography" (request 5); and "[a]ny and all policies, procedures, reports, guidelines, manuals, or other materials, regarding the discovery, review, and/or reporting of accounts for suspected child pornography by Microsoft, whether manual or automated; . . . and, any communications with employees regarding user/subscriber content to be flagged" (request 10, in relevant part). Based on our conversation, we understand that these requests go to your private search doctrine argument. We further understand that your position is, under *Wilson*, the "who what when" of a private party search is relevant to determining the scope of the search. Because Microsoft does not retain specific "who what when" records on the review of any given image, we understand your thinking is that policies, guidelines, training materials, etc. might contain information explaining how reviews are typically handled, which would inform the private search doctrine analysis.

As we laid out in our prior e-mail, "Rule 17 'was not intended to provide a means of discovery for criminal cases[,]' [and thus] Rule 17 subpoenas may not be used to engage in a general 'fishing expedition.'" *US v. Omidi*, 2021 WL 7629899, at *2 (C.D. Cal. May 20, 2021) (quoting *United States v. Nixon*, 418 U.S. 683, 698-700 (1974)). Rather, a party seeking evidence pursuant to a Rule 17 subpoena "must clear three hurdles: (1) relevancy; (2) admissibility; (3) specificity." *Nixon*, 418 U.S. at 700.

As for specificity, courts in the 9th Circuit have repeatedly held that "the movant must request specific documents and not entire categories of files" because "Rule 17(c) was not intended to 'allow a blind fishing expedition seeking unknown evidence.'" *United States v. Smith*, 2020 WL 5763841, at *1 (E.D. Cal. Sept. 28, 2020) (quoting *US v. Reed*, 726 F.2d 570, 577 (9th Cir. 1984)). Accordingly, "broad and sweeping" requests seeking "any and all" documents falling into a particular category fail the specificity requirement. *Omdi,* 2021 WL 7629899, at *2. Requests 5 and 10 are precisely the type of "broad and sweeping" "any and all" requests that are not permitted under Rule 17 -- every record from July 2019 related to Microsoft's policies, procedures, training, etc. in connection with reporting suspected child pornography hardly amounts to a "sharply defined group of documents," as required by the Rule. *See US v. Shepard*, 2010 WL 750110, at *1 (E.D. Mo. Feb. 26, 2010) (emphasis added). Rather, these are "entire categories of files" which cannot be obtained with a Rule 17 subpoena.

As for relevance and admissibility, there "must be a substantial foundation for the movant's belief that the requested material exists and will be relevant and admissible." *Smith*, 2020 WL 5763841, at *1 (citing *Reed*, 726 F.2d at 577). "[B]road requests for documents in the mere hope that they will contain exculpatory material [] amounts to little more than a blind fishing expedition" and fail Rule 17's relevance and admissibility requirements. *United States v. Johnson*, 2014 WL 6068089, at *6–7 (N.D. Cal. Nov. 13, 2014) (quotations omitted).

Here, requests 5 and 10 fail the relevance and admissibility requirements for multiple reasons. First, we understand that your requests are motivated by the thought that they may "have some potential for relevance and evidentiary use," depending on what they say about standard practice for reporting child pornography -- this is not enough to justify a Rule 17 request. *See US v. Roque*, 2014 WL 12691605, at *2 (C.D. Cal. Aug. 18, 2014). Moreover, we do not see how information regarding Microsoft's standard practice for reporting child pornography would have any relevance to the Fourth Amendment analysis here in the first place. The case law is clear that "Fourth Amendment cases must be decided on the facts of each case, not by . . . generalizations." *Dow Chem. Co. v. United States*, 476 U.S. 227, 238 n.5 (1986), *see also Maryland v. Macon*, 472 U.S. 463, 470–71 (1985) ("Whether a Fourth Amendment violation has occurred turns on an objective assessment of the officer's actions in light of the facts and circumstances confronting him at the time . . . ."). Private search doctrine cases are no different: what matters is the actual conduct of the private party and the government. *See United States v. Lichtenberger*, 786 F.3d 478 (6th Cir. 2015) ("As with any Fourth Amendment case, the facts underlying the *Jacobsen* case are key to its holding."). Even *Wilson* -- the case the defendant is relying on -- stresses this point, explaining that Google's prior actions were "not pertinent to whether a private search eroded *Wilson's* expectation of privacy." *United States v. Wilson*, 13 F.4th 961, 979 (9th Cir. 2021). In light of this framework, courts in the 9th Circuit have rejected Rule 17 requests for police manuals, protocols, and the like in connection with suppression hearings, because "[t]he instructions given to [] officers, as well as their motivation for [conducting the search], are not relevant to the Fourth Amendment analysis that [the] Court must undertake to resolve [a] motion to suppress." *United States v. Johnson*, 2014 WL 6068089, at *6–7 (N.D. Cal. Nov. 13, 2014); *cf. United States v. Robinson*, 2019 WL 6255475, at *2 (D. Idaho Nov. 22, 2019) (rejecting Rule 16 request for police policy and training documents as irrelevant to an upcoming suppression hearing). Likewise, documents reflecting Microsoft's typical procedure for reviewing suspected child pornography have no bearing on the scope of the *actual* review that occurred, nor would they inform the fact-specific analysis that the Court must undertake in its suppression hearing. Accordingly, even if the requested materials contain the information the defendant is seeking, that information would not be relevant or admissible at the suppression hearing, and therefore cannot be obtained under Rule 17.

For the foregoing reasons, we are confident that requests 5 and 10 (in relevant part) far exceed the scope of Rule 17, and would be quashed by the Court. That said, as we discussed yesterday, Microsoft would prefer to avoid litigation on these requests and would welcome your thoughts on a potential resolution, including if there is anything Microsoft can add to the declaration that would resolve these outstanding issues.

I'd welcome your reactions. If you think another call would be productive, I'm happy to schedule one.

Best,

Megan

From: Gabriela Bischof <Gabriela_Bischof@fd.org>
Sent: Friday, March 17, 2023 1:39 PM
To: Crowley, Megan <MCrowley@cov.com>; Karthik Raju <Karthik_Raju@fd.org>
Cc: Goodwin, Chloe <CGoodwin@cov.com>; Fitch, James <JHFitch@cov.com>; Robert Ultan <Robert_Ultan@fd.org>
Subject: Re: United States v. Burley, No. 21-CR-00198 EMC

[EXTERNAL]

Hi Megan,

Thanks for your email. Are you free Monday at noon Pacific? We could talk then.

Thanks,

Gabriela

From: Crowley, Megan <MCrowley@cov.com>
Sent: Thursday, March 16, 2023 6:16:27 PM
To: Karthik Raju
Cc: Goodwin, Chloe; Fitch, James; Gabriela Bischof; Robert Ultan
Subject: RE: United States v. Burley, No. 21-CR-00198 EMC

EXTERNAL SENDER

Hi Karthik and Gabriella,

Thanks for your reply, and for your agreement with our proposals for requests 1, 3, 7-9, and 11, subject to the caveat that our use of the term "documents" encompasses records beyond Word or PDF documents, to include the record types contemplated by Federal Rule of Criminal Procedure 17(c) ("books, papers, documents, data, or other objects").

As for the remaining requests (2, 4-6, and 10), we view them to be outside the scope of Rule 17. It is well established that "Rule 17 'was not intended to provide a means of discovery for criminal cases[,]' [and thus] Rule 17 subpoenas may not be used to engage in a general 'fishing expedition.'" *US v. Omidi*, 2021 WL 7629899, at *2 (C.D. Cal. May 20, 2021) (quoting *United States v. Nixon*, 418 U.S. 683, 698-700 (1974)). Rather, a party seeking evidence pursuant to a Rule 17 subpoena "must clear three hurdles: (1) relevancy; (2) admissibility; (3) specificity." *Nixon*, 418 U.S. at 700.

Courts in the 9th Circuit have repeatedly held that "the movant must request specific documents and not entire categories of files" because "Rule 17(c) was not intended to 'allow a blind fishing expedition seeking unknown evidence.'" *United States v. Smith*, 2020 WL 5763841, at *1 (E.D. Cal. Sept. 28, 2020) (quoting *US v. Reed*, 726 F.2d 570, 577 (9th Cir. 1984)); *see also Omidi*, 2021 WL 7629899, at *2 ("broad and sweeping" requests seeking "any and all" documents falling into a particular category fail the specificity requirement). These requests also tend to fail the

relevance and admissibility requirement, because the defendant must "show . . . the relevance and admissibility of *all of the materials sought in the [s]ubpoena*" including *all* of the documents that fall under a broad "any and all" request. *Omidi*, 2021 WL 7629899, at *2. "It is not enough [to] have some potential for relevance and evidentiary use." *US v. Roque*, 2014 WL 12691605, at *2 (C.D. Cal. Aug. 18, 2014). Moreover, 9th Circuit courts have held that there "must be a substantial foundation for the movant's belief that the requested material exists and will be relevant and admissible." *Smith*, 2020 WL 5763841, at *1 (citing *Reed*, 726 F.2d at 577). "[S]uspicion" that requested material "may exist" is not enough, as this "falls short of establishing a 'substantial foundation' for such a belief." *Id.* at *2.

Under this well-established law, requests 2, 4-6, and 10 seek records outside the scope of Rule 17. Requests 4, 5, 6, and 10 are the type of broad "any and all" requests for "entire categories of files" that fail Rule 17's specificity requirement. Instead of specifically identifying the documents sought, these requests seek entire categories of records. For similar reasons, these requests fail the relevance and admissibility requirement. Rather, these appear to be discovery-like requests to "see what may turn up."

Separately, we struggle to see how even a more narrow set of documents of the kind sought under requests 4, 5, 6, and 10 could be relevant to a motion to suppress -- for example, we can see no reason why any materials used to train Microsoft employees on the definitions of child pornography could have relevance to the Fourth Amendment analysis here.

You also state that you do not waive your requests for "proprietary" information responsive to your subpoena even where public information has already been provided. But seeking additional, non-public information would be cumulative to public information, and "Rule 17 subpoenas should . . . be quashed when they seek cumulative" information. *US v. Espinoza*, 641 F.2d 153, 159 (4th Cir. 1981).

Finally, for clarity, we reiterate that Microsoft does not view itself as being subject to any non-disclosure obligation in connection with your subpoena.

We think it might be helpful to schedule a call as a next step. Would you be available to discuss further tomorrow?

Best,

Megan

From: Karthik Raju <Karthik_Raju@fd.org>
Sent: Tuesday, March 14, 2023 8:15 PM
To: Crowley, Megan <MCrowley@cov.com>
Cc: Goodwin, Chloe <CGoodwin@cov.com>; Fitch, James <JHFitch@cov.com>; Gabriela Bischof <Gabriela_Bischof@fd.org>; Robert Ultan <Robert_Ultan@fd.org>
Subject: United States v. Burley, No. 21-CR-00198 EMC

[EXTERNAL]

Hi Megan,

Thanks for your response. We'll share some broader concerns and then comment on your replies to our individual requests.

I hope that you understand that because this is a criminal case, our ethical duties to our client do not allow us to negotiate away requests for information relevant to his case. That said, we will continue to move forward in good faith to ensure that compliance with the subpoena is as minimally burdensome as possible.

We have two broad concerns regarding the production of documents vs. the production of information. We want to flag that our subpoena seeks information, not merely documents. I want to be sure that where your responses refer only to documents, it is also inclusive of other forms of information.

Secondly, in several places, your response directs us to publicly available information. If there is proprietary information that is responsive to our subpoena, we do not waive our request for that information. Instead, we request that Microsoft submit this information in camera to the Court and request a protective order. We have no objection to any reasonable protective order for proprietary or other sensitive information, such as training materials, employee access logs, etc.

Requests

1. All materials, including reports, emails, documents, or other written and unwritten materials, related to the CyberTip report (CT # 52016239) submitted by Microsoft to NCMEC and law enforcement agencies including the entire contents of that report.

   Response: As part of an overall agreement relating to reasonable scope limitations on your subpoena, Microsoft would be willing to conduct a reasonable search for documents pertaining to the Cybertip at issue in this case.

Reply: Per the concern stated above, this response limits Microsoft's obligation to conduct a reasonable search for "documents". We ask that you kindly confirm that the search will include all responsive information, not just documents.

2. A detailed description of the method(s) by which image files were located by Microsoft, including but not limited to the manner in which hash values are assigned to the original photographs and the images deemed to replicate them and any validation studies or other information regarding the reliability of Microsoft's programs in identifying such original images and images deemed to replicate them.

Response: We have shared public information regarding the functioning of PhotoDNA. We view the remainder of this request as written as outside the bounds of Microsoft's Rule 17 obligations.

Reply: We reiterate that do not waive our request for the specific information requested simply because Microsoft states that it has "shared public information" purportedly responsive to the request. In this instance, however, per our conversation, we would request an affirmative statement that Microsoft has not conducted its own validation studies. Similarly, assuming the method of locating CSAM and assigning hash values as described in Davis' declaration in Bohannon remains unchanged, we request a declaration specific to this case.

3. Any documentation and description related to CyberTip # 52016239 of all actions Microsoft undertook in relation to the images and/or associated Skype chats or file storage, before reporting them to NCMEC, including but not limited to whether an employee at Microsoft reviewed one or more of the four images contained in the CyberTip Report, the identity of the Microsoft employee(s) who viewed the images; which image they each viewed, when they viewed the images, the identity of the employee who submitted the report and files to NCMEC and when, and all records, in any form, that memorialize any and all of these actions.

Response: We have shared public information responsive to this request. Additionally, as part of an overall agreement relating to reasonable scope limitations on your subpoena, Microsoft would be willing to conduct a reasonable search for documents pertaining to the Cybertip at issue in this case.

Reply: We reaffirm our request for all specific information asked for in this request, and for information on the specific steps taken by Microsoft pertinent to CyberTip 52016239. We ask that Microsoft affirm that any "reasonable search" for materials responsive to this request include information and not merely documents.

4. Any records and information, in any form, pertaining to whether Microsoft has used an automated system, not requiring a Microsoft employee, to generate and submit CyberTip reports with NCMEC, including the dates

when such an automated system was in effect. If Microsoft used such an automated system at the time of the CyberTip referenced above, please provide a detailed description of the system etc.

Response: We have shared public information responsive to this request. Additionally, as part of an overall agreement relating to reasonable scope limitations on your subpoena, Microsoft would be willing to conduct a reasonable search for documents pertaining to the Cybertip at issue in this case.

Reply: We again request that a search for the requested materials include information and not only documents. We ask for an affirmation responsive to whether Microsoft ever used an automated reporting system at a time previous to Cybertip 52016239 and whether any such system was in effect at the time of Cybertip 52016239 was communicated.

5. Any training materials used to train Microsoft employees on the definitions of child pornography, company reporting procedures for located suspected child pornography, classification standards of suspected child pornography.

Response: We have shared public information describing the steps that Microsoft takes if the hash of scanned content matches the hash of a known image of child sexual abuse. We view the remainder of this request as outside the bounds of Microsoft's Rule 17 obligations.

Reply: We maintain our request for the specific information sought in this request. We reiterate that we are willing to accept responsive information subject to a reasonable protective order. Should Microsoft continue to maintain that it will not provide further information, we ask that Microsoft specifically elaborate which materials it views as being outside the scope of Rule 17 and why they fall outside of Microsoft's Rule 17 obligations.

6. Any reports, emails, documents or other written and unwritten materials describing or related to any automated reporting system used at any time by Microsoft to report suspected child pornography to NCMEC and/or police agencies. If Microsoft does not possess any of these materials, information as to whether Microsoft ever used an automated reporting system and when.

Response: Same response as #5.

Reply: We maintain our request for this information, but we are willing to narrow the time frame to July 30, 2018, to January 13, 2020 as relevant to CyberTip 52016239.

7. All correspondence, in any form, to NCMEC, Microsoft, or law enforcement agencies from Microsoft's PhotoDNA program, or the API associated with the PhotoDNA program, related to the CyberTip report referenced above.

Response: As part of an overall agreement relating to reasonable scope limitations on your subpoena, Microsoft would be willing to conduct a reasonable search for documents pertaining to the CyberTip at issue in this case.

Reply: We request that Microsoft's search include information in addition to documents.

8. All materials, including reports, emails, documents, or other written and unwritten materials, in Microsoft's possession, custody or control related to NCMEC's response to the CyberTip report identified above, including all actions taken by NCMEC with respect to any information received from Microsoft, such as opening any emails, opening any attachments, conducting any investigation, and forwarding any information to law enforcement.

Response: As part of an overall agreement relating to reasonable scope limitations on your subpoena, Microsoft would be willing to conduct a reasonable search for documents pertaining to the CyberTip at issue in this case.

Reply: We request that Microsoft's search include information in addition to documents.

9. Any and all policies and procedures, reports, guidelines, manuals, operating agreements, letters of understanding, memoranda, meeting notes or other materials, regarding Microsoft's reporting to, and relationship with NCMEC, the federal Department of Justice including the Federal Bureau of Investigation, the Santa Rosa Police Department, the Sonoma County Sheriff's Office, or any other state and local law enforcement, including but not limited to:
    a. All correspondence between NCMEC and Microsoft concerning requests NCMEC made to Microsoft to sign up for its CyberTip line.
    b. Documents sufficient to show any request NCMEC sent to or received from Microsoft concerning Microsoft's PhotoDNA program addressing the financing or technical development of the PhotoDNA software or any associated API, or NCMEC's specific needs or software requirements to run the program or any associated API.
    c. All registration materials related to the registration of Microsoft or Microsoft's subsidiary PhotoDNA for NCMEC's CyberTip line.
    d. All of NCMEC's Memoranda of Understanding or similar agreements with Microsoft addressing the sharing of NCMEC's library or platform of hash values associated with contraband.
    e. Any communications between Microsoft and any law enforcement agency concerning Microsoft's investigation into Cian Burley or CyberTip # 52016239.

Response: Microsoft would be prepared to conduct a reasonable search for any agreements or MOUs relating to PhotoDNA with NCMEC, the U.S. Department of Justice, the Federal Bureau of Investigation, the Santa Rosa

Police Department, and the Sonoma County Sheriff's Office that were operative at the time of the CyberTip at issue in this case.

Reply: We request that Microsoft's search include information in addition to documents.

10. Any and all policies, procedures, reports, guidelines, manuals, or other materials, regarding the discovery, review, and/or reporting of accounts for suspected child pornography by Microsoft, whether manual or automated; a description of any technology or methods used to search user data, including PhotoDNA and/or similar technologies or methods; and, any communications with employees regarding user/subscriber content to be flagged.

Response: We have shared public information describing the steps that Microsoft takes if the hash of scanned content matches the hash of a known image of child sexual abuse. We view the remainder of this request as outside the bounds of Microsoft's Rule 17 obligations.

Reply: We are willing to narrow this request to responsive materials specifically relating to CyberTip 52016239 and its investigation. To the extent Microsoft maintains this information is not covered by its Rule 17 obligations, we request a statement detailing its specific Rule 17 objections.

11. Microsoft's Privacy Policy and Terms of Service in effect from July 30, 2018, to January 13, 2020.

Response: Microsoft would agree to produce materials responsive to this request.

Reply: Thank you.

In terms of whether Microsoft is under any sort of legal restraint to not speak with others about our subpoena, we cannot advise you of your obligations and would simply direct you to the subpoena itself, which does not provide for disclosure to the Government. As well, we wish to remind Microsoft that the correct tip number is CyberTip 52016239.

We are happy to discuss any questions or issues at a mutually convenient time.

Thanks,

Karthik Raju/Gabriella Bischof

Exhibit C

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN®

CyberTipline Report 52016239

Priority Level: E
(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 07-09-2019 02:01:21 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief overview of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

NCMEC Incident Type is based on NCMEC's review of the report **OR** a "Hash Match" of one or more uploaded files. NCMEC may not have viewed all uploaded files submitted by the reporting ESP.

NCMEC staff have viewed one or more of the files submitted with this CyberTipline report and have categorized one or more of the files as designated in the Incident Type.

Please see Section C for additional information related to the files that were viewed and categorized by NCMEC.

Total Uploaded Files: 4

Contents

Section A: Reported Information

The following information was submitted to the CyberTipline by the Reporting Person or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - Online Operations
Microsoft Microsoft Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Company Information

U.S. Law Enforcement - Where to serve Legal Process in Criminal Matters

OneDrive, Skype, Xbox, BingImage and other Microsoft Online Services:

Microsoft Corporation
Attn: Custodian of Records
One Microsoft Way
Redmond, WA 98052
Service of Process Only: uslereq@microsoft.com
Inquiries Only: msndcc@microsoft.com

Emergency Requests
Microsoft responds to emergency requests, 24 hours a day, if it relates to the imminent threat of death or serious physical injury as permitted in 18 U.S.C. section 2702(b)(8) and (c)(4). If you have an emergency request, please call the Law Enforcement National Security (LENS) hotline at (425) 722-1299. You may also submit an emergency request via e-mail to lealert@microsoft.com.

Non-U.S. Law Enforcement
Microsoft has established local contacts within your country/region to handle your legal process. If you are not already familiar with your local contact, send an email to globalcc@microsoft.com and you will be directed to the contact handling requests from your country/region. Your local contact will educate you as to what local process must be followed to obtain customer account records. All legal process from non-U.S. law enforcement/prosecutors/courts must be directed to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 U.S.A. Do not direct your legal process to a local subsidiary of Microsoft.

Incident Information

Incident Type:	Child Pornography (possession, manufacture, and distribution)
Incident Time:	07-05-2019 18:13:53 UTC
Description of Incident Time:	Incident Time reflects when first image/video in the series was scanned

Peer to Peer

Peer-to-Peer Client:	Skype
IP Address:	68.123.8.91 at 07-05-2019 18:13:53 UTC
Peer to Peer Filenames:	2bf5b62d-9c6f-40ee-abdd-744c59b562f9.jpg

Peer to Peer

Peer-to-Peer Client:	Skype
IP Address:	68.123.8.91 at 07-05-2019 18:31:45 UTC
Peer to Peer Filenames:	17a9ae23-8fb4-4c98-8e86-bb732c818fa7.jpg

Peer to Peer

Peer-to-Peer Client:	Skype
IP Address:	68.123.8.91 at 07-05-2019 18:35:38 UTC
Peer to Peer Filenames:	f0824379-e294-432e-b37f-1cdbcadb7180.jpg

Peer to Peer

Peer-to-Peer Client:	Skype
IP Address:	68.123.8.91 at 07-05-2019 18:41:59 UTC
Peer to Peer Filenames:	527789f4-ac96-4f97-8a4a-284cc7be8db7.jpg

Suspect

Screen/User Name:	live:ciank111980
IP Address:	68.123.8.91 07-05-2019 18:13:53 UTC
IP Address:	68.123.8.91 07-05-2019 18:31:45 UTC
IP Address:	68.123.8.91 07-05-2019 18:35:38 UTC
IP Address:	68.123.8.91 07-05-2019 18:41:59 UTC
Additional Information:	DocumentId: 0-cus-d6-44f9dbeedeb05e4f64bbf5d8aa61adc0 Please provide ScreenName and DocumentId when requesting more information from Microsoft.

Uploaded File Information

Number of uploaded files:	4

Uploaded File Information

Filename:	2bf5b62d-9c6f-40ee-abdd-744c59b562f9.jpg
MD5:	7352f0a58d20e2736fc866cba2832bb8
Submittal ID:	b9fc8e1f130e8cc0bd20f2eb54891015
Did Reporting ESP view entire contents of uploaded file?	Yes

Did Reporting ESP view the EXIF of uploaded file?	(Information Not Provided by Company)
Were entire contents of uploaded file publicly available?	(Information Not Provided by Company)
Image Categorization by ESP: (See Section B for further explanation)	A2
Original Binary Hash of File (PhotoDNA):	50,0,0,26,31,30,10,58,22,153,5,213,101,28,9,237,45,11,8,83,0,14,0,29,89,4,0,71,39,131,88,122,25,236,103,151,243,34,79,108,92,13,54,49,1,18,0,33,124,0,0,102,95,38,25,73,38,255,67,57,255,30,43,37,40,23,2,27,1,22,0,26,145,0,14,48,133,43,16,41,70,249,82,32,219,53,86,21,50,25,15,9,0,26,9,7,115,0,148,4,114,19,104,4,79,217,90,6,184,61,71,4,46,30,91,2,8,13,115,4,57,1,71,33,52,16,44,38,45,161,66,41,147,43,67,20,46,2,32,35,15,0,43,48
Original URL Where File was Located:	https://nus1-storage.asm.skype.com:444/v1/objects/0-cus-d6-44f9dbeedeb05e4f64bbf5d8aa61adc0/content/imgpsh

Source Information:

Type	Value	Event	Date/Time
IP Address	68.123.8.91		07-05-2019 18:13:53 UTC

Uploaded File Information

Filename:	f0824379-e294-432e-b37f-1cdbcadb7180.jpg
MD5:	a82d38264e764cb2694581801f55aff4
Submittal ID:	c51eaeaee688f59abbc26f8f7ebc3aa1
Did Reporting ESP view entire contents of uploaded file?	Yes
Did Reporting ESP view the EXIF of uploaded file?	(Information Not Provided by Company)
Were entire contents of uploaded file publicly available?	(Information Not Provided by Company)
Image Categorization by ESP: (See Section B for further explanation)	B2
Original Binary Hash of File (PhotoDNA):	32,85,58,81,46,32,35,62,56,47,37,69,61,137,124,59,41,141,73,116,149,41,34,154,85,55,96,44,73,150,144,79,93,60,131,94,105,93,126,120,21,158,212,18,197,57,174,31,95,46,72,41,51,129,70,39,113,46,103,55,71,129,91,89,125,94,75,62,88,148,107,74,57,39,49,73,31,95,34,47,93,52,44,59,48,121,58,62,126,69,52,60,56,84,94,97,95,60,74,44,49,143,51,62,146,53,59,65,51,88,98,17,81,72,86,28,72,113,118,57,14,7,12,9,17,99,45,33,127,43,63,54,50,82,33,147,74,43,13,118,7,17,24,9
Original URL Where File was Located:	https://nus1-storage.asm.skype.com:444/v1/objects/0-cus-d10-24604fa047f70d6d7f92583667dd66d8/content/imgpsh

Source Information:

Type	Value	Event	Date/Time
IP Address	68.123.8.91		07-05-2019 18:35:38 UTC

Uploaded File Information

Filename:	17a9ae23-8fb4-4c98-8e86-bb732c818fa7.jpg
MD5:	8d293bc6aaf098ba783be853dbe6c0ba
Submittal ID:	d94a67759c4bf03e20ff02e79cc44e60

Did Reporting ESP view entire contents of uploaded file?	Yes
Did Reporting ESP view the EXIF of uploaded file?	(Information Not Provided by Company)
Were entire contents of uploaded file publicly available?	(Information Not Provided by Company)
Image Categorization by ESP: (See Section B for further explanation)	B2
Original Binary Hash of File (PhotoDNA):	42,41,128,11,114,27,238,30,46,48,73,77,54,17,61,45,24,76,76,37,44,161,54,119,53,44,15,121,107,46,21,177,89,69,38,97,91,44,40,53,26,134,17,139,19,187,19,140,19,60,12,79,107,17,32,114,103,30,25,108,75,75,9,144,2,149,31,157,7,78,39,78,15,82,14,113,162,14,48,124,92,105,30,100,102,110,29,173,6,121,27,142,10,93,44,118,63,57,43,42,136,15,75,46,78,113,109,100,99,88,139,64,8,110,54,18,25,41,39,22,77,47,36,124,151,15,43,113,79,63,92,146,81,79,52,146,16,138,52,24,24,53,12,50
Original URL Where File was Located:	https://nus1-storage.asm.skype.com:444/v1/objects/0-cus-d5-d99abad216610b9d8c0fa759acc364e0/content/imgpsh

Source Information:

Type	Value	Event	Date/Time
IP Address	68.123.8.91		07-05-2019 18:31:45 UTC

Uploaded File Information

Filename:	527789f4-ac96-4f97-8a4a-284cc7be8db7.jpg
MD5:	0b4c1d2bc6e858affe39aae81989c9aa
Submittal ID:	7b8651a82b379da9057581c80e92416f
Did Reporting ESP view entire contents of uploaded file?	Yes
Did Reporting ESP view the EXIF of uploaded file?	(Information Not Provided by Company)
Were entire contents of uploaded file publicly available?	(Information Not Provided by Company)
Image Categorization by ESP: (See Section B for further explanation)	B1
Original Binary Hash of File (PhotoDNA):	136,162,171,78,174,133,173,68,81,68,195,84,52,81,178,57,79,110,193,49,109,94,166,32,112,162,105,101,140,88,139,74,104,120,98,95,119,67,79,81,85,133,116,88,114,98,107,65,108,81,135,74,70,62,95,36,54,61,113,53,74,65,112,53,49,58,98,58,59,48,82,39,57,51,28,90,46,46,56,57,30,77,30,88,51,58,16,97,62,45,34,106,75,57,39,84,77,51,50,72,54,45,36,102,32,64,32,56,47,41,60,44,53,48,45,46,99,28,94,71,79,27,43,39,50,70,81,37,42,72,40,65,62,36,47,56,41,40,51,34,75,41,28,111
Original URL Where File was Located:	https://nus1-storage.asm.skype.com:444/v1/objects/0-cus-d9-e983dc91be69eb630b9f02d200842093/content/imgpsh

Source Information:

Type	Value	Event	Date/Time
IP Address	68.123.8.91		07-05-2019 18:41:59 UTC

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of

the Reporting Person or Reporting ESP.

Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "Suspect," NCMEC Systems will geographically resolve the IP address via a publicly-available online query. The results of this lookup are displayed.

Geolocation data is approximate and may not display a user's exact location. Please be aware that the geolocation information provided is not exact but is providing a reliable estimate of location based on IP address(es) voluntarily provided by the reporting ESP.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A2: 1
B1: 1
B2: 2

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Suspect)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
68.123.8.91	US	CA	Santa Rosa	San Francisco-Oakland-San Jose	95401		38.4426/ -122.7547	AT&T Internet Services/ AT&T Internet Services

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
68.123.8.91	US	CA	Santa Rosa	San Francisco-Oakland-San Jose	95401		38.4426/ -122.7547	AT&T Internet Services/ AT&T Internet Services

This concludes Section B

Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from queries on publicly-available, open-source websites. Any queries conducted by NCMEC staff will be documented and any query results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification*:	Apparent Child Pornography
International Country:	United States
NCMEC Date Processed:	08-07-2019 20:00:39 UTC
Made Available to Law Enforcement by NCMEC:	Yes

NCMEC Classification is based on NCMEC's review of the report **OR** a "Hash Match" of one or more uploaded files. NCMEC may not have viewed all uploaded files submitted by the reporting ESP.

NCMEC Note #1

ECD-SEV 08-07-2019 20:00:39 UTC

I reviewed the uploaded files and found what appears to be CHILD PORNOGRAPHY.

=====

CT/TA queries for the following yielded negative or irrelevant results:
68.123.8.91
ciank111980

=====

Spokeo, Google, Instagram, Twitter, and Kik for ciank111980 returned negative results

=====

Based on the reported IP address, I have sent this report to the San Jose ICAC

Uploaded File Information

Files Viewed by NCMEC:

NCMEC staff have viewed the following uploaded files which had not been previously viewed and categorized by NCMEC at the time this report was generated.

Files Viewed by NCMEC

Filename	MD5
2bf5b62d-9c6f-40ee-abdd-744c59b562f9.jpg	7352f0a58d20e2736fc866cba2832bb8
f0824379-e294-432e-b37f-1cdbcadb7180.jpg	a82d38264e764cb2694581801f55aff4
17a9ae23-8fb4-4c98-8e86-bb732c818fa7.jpg	8d293bc6aaf098ba783be853dbe6c0ba

Files Viewed by NCMEC

Filename	MD5
527789f4-ac96-4f97-8a4a-284cc7be8db7.jpg	0b4c1d2bc6e858affe39aae81989c9aa

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.

Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

San Jose Police Department

Investigator:

Assigned Officer:	Access VPN
Title:	Det. Chiristian Mendoza
City/State:	San Jose, CA
Country:	United States
Phone Number:	408-896-3079
Email Address:	christian.mendoza@sanjoseca.gov,jose.montoya@sanjoseca.gov,michael.ogrady@sanjoseca.gov,sean.pierce@sanjoseca.gov

Time/Date was made available: 08-07-2019 20:00:39 UTC

This concludes Section D

This concludes CyberTipline Report 52016239

Exhibit D

From: Crowley, Megan
Sent: Wednesday, March 8, 2023 8:27 PM
To: Gabriela Bischof; Robert Ultan; Fitch, James
Cc: Goodwin, Chloe; Karthik Raju; Fitch, James
Subject: RE: United States v. Burley, No. 21-CR-00198 EMC

Hi Gabriela,

Further to our conversation on Monday and my email on Tuesday, we are writing to provide further detail in response to your requests.

As we discussed, Microsoft is a third party to this matter, and Rule 17 is not a means for conducting discovery. Although Microsoft is willing to accommodate certain of your requests (as set out below), we remain concerned that many of the requests as written are overbroad, unduly burdensome, and disproportionate to the needs of your case. With that said, the following are our responses to each of your requests, which are consistent with prior judicial decisions regarding the scope of Microsoft's Rule 17 obligations in similar cases:

1. All materials, including reports, emails, documents, or other written and unwritten materials, related to the CyberTip report (CT # 56016239) submitted by Microsoft to NCMEC and law enforcement agencies including the entire contents of that report.

   Response: As part of an overall agreement relating to reasonable scope limitations on your subpoena, Microsoft would be willing to conduct a reasonable search for documents pertaining to the Cybertip at issue in this case.

2. A detailed description of the method(s) by which image files were located by Microsoft, including but not limited to the manner in which hash values are assigned to the original photographs and the images deemed to replicate them and any validation studies or other information regarding the reliability of Microsoft's programs in identifying such original images and images deemed to replicate them.

   Response: We have shared public information regarding the functioning of PhotoDNA. We view the remainder of this request as written as outside the bounds of Microsoft's Rule 17 obligations.

3. Any documentation and description related to CyberTip # 56016239 of all actions Microsoft undertook in relation to the images and/or associated Skype chats or file storage, before reporting them to NCMEC, including but not limited to whether an employee at Microsoft reviewed one or more of the four images contained in the CyberTip Report, the identity of the Microsoft employee(s) who viewed the images; which image they each viewed, when they viewed the images, the identity of the employee who submitted the report and files to NCMEC and when, and all records, in any form, that memorialize any and all of these actions.

   Response: We have shared public information responsive to this request. Additionally, as part of an overall agreement relating to reasonable scope limitations on your subpoena, Microsoft would be willing to conduct a reasonable search for documents pertaining to the Cybertip at issue in this case.

4. Any records and information, in any form, pertaining to whether Microsoft has used an automated system, not requiring a Microsoft employee, to generate and submit CyberTip reports with NCMEC, including the dates when such an automated system was in effect. If Microsoft used such an automated system at the time of the CyberTip referenced above, please provide a detailed description of the system etc.

   Response: We have shared public information responsive to this request. Additionally, as part of an overall agreement relating to reasonable scope limitations on your subpoena, Microsoft would be willing to conduct a reasonable search for documents pertaining to the Cybertip at issue in this case.

5. Any training materials used to train Microsoft employees on the definitions of child pornography, company reporting procedures for located suspected child pornography, classification standards of suspected child pornography.

   Response: We have shared public information describing the steps that Microsoft takes if the hash of scanned content matches the hash of a known image of child sexual abuse. We view the remainder of this request as outside the bounds of Microsoft's Rule 17 obligations.

6. Any reports, emails, documents or other written and unwritten materials describing or related to any automated reporting system used at any time by Microsoft to report suspected child pornography to NCMEC and/or police agencies. If Microsoft does not possess any of these materials, information as to whether Microsoft ever used an automated reporting system and when.

   Response: Same response as #5.

7. All correspondence, in any form, to NCMEC, Microsoft, or law enforcement agencies from Microsoft's PhotoDNA program, or the API associated with the PhotoDNA program, related to the CyberTip report referenced above.

   Response: As part of an overall agreement relating to reasonable scope limitations on your subpoena, Microsoft would be willing to conduct a reasonable search for documents pertaining to the Cybertip at issue in this case.

8. All materials, including reports, emails, documents, or other written and unwritten materials, in Microsoft's possession, custody or control related to NCMEC's response to the CyberTip report identified above, including all actions taken by NCMEC with respect to any information received from Microsoft, such as opening any emails, opening any attachments, conducting any investigation, and forwarding any information to law enforcement.

   Response: As part of an overall agreement relating to reasonable scope limitations on your subpoena, Microsoft would be willing to conduct a reasonable search for documents pertaining to the Cybertip at issue in this case.

9. Any and all policies and procedures, reports, guidelines, manuals, operating agreements, letters of understanding, memoranda, meeting notes or other materials, regarding Microsoft's reporting to, and relationship with NCMEC, the federal Department of Justice including the Federal Bureau of Investigation, the Santa Rosa Police Department, the Sonoma County Sheriff's Office, or any other state and local law enforcement, including but not limited to:
   a. All correspondence between NCMEC and Microsoft concerning requests NCMEC made to Microsoft to sign up for its CyberTip line.
   b. Documents sufficient to show any request NCMEC sent to or received from Microsoft concerning Microsoft's PhotoDNA program addressing the financing or technical development of the PhotoDNA software or any associated API, or NCMEC's specific needs or software requirements to run the program or any associated API.
   c. All registration materials related to the registration of Microsoft or Microsoft's subsidiary PhotoDNA for NCMEC's CyberTip line.
   d. All of NCMEC's Memoranda of Understanding or similar agreements with Microsoft addressing the sharing of NCMEC's library or platform of hash values associated with contraband.
   e. Any communications between Microsoft and any law enforcement agency concerning Microsoft's investigation into Cian Burley or CyberTip # 56016239.

   Response: Microsoft would be prepared to conduct a reasonable search for any agreements or MOUs relating to PhotoDNA with NCMEC, the U.S. Department of Justice, the Federal Bureau of Investigation, the Santa Rosa Police Department, and the Sonoma County Sheriff's Office that were operative at the time of the Cybertip at issue in this case.

10. Any and all policies, procedures, reports, guidelines, manuals, or other materials, regarding the discovery, review, and/or reporting of accounts for suspected child pornography by Microsoft, whether manual or automated; a description of any technology or methods used to search user data, including PhotoDNA and/or similar technologies or methods; and, any communications with employees regarding user/subscriber content to be flagged.

    Response: We have shared public information describing the steps that Microsoft takes if the hash of scanned content matches the hash of a known image of child sexual abuse. We view the remainder of this request as outside the bounds of Microsoft's Rule 17 obligations.

11. Microsoft's Privacy Policy and Terms of Service in effect from July 30, 2018, to January 13, 2020.

    Response: Microsoft would agree to produce materials responsive to this request.

Please let us know if you agree to this proposal to resolve your subpoena. If you do, we can send you a draft proposed protective order and confirm when we would be able to produce these materials.

Thanks,
Megan

From: Crowley, Megan
Sent: Tuesday, March 7, 2023 12:13 PM
To: 'Gabriela Bischof' <Gabriela_Bischof@fd.org>; Robert Ultan <Robert_Ultan@fd.org>; Fitch, James <JHFitch@cov.com>
Cc: Goodwin, Chloe <CGoodwin@cov.com>; Karthik Raju <Karthik_Raju@fd.org>; Fitch, James <JHFitch@cov.com>
Subject: RE: United States v. Burley, No. 21-CR-00198 EMC

Gabriela,

Thank you for the call yesterday. I am sending this email to share some information that I hope resolves some of your requests, as well as to summarize our conversation concerning next steps.

The following public information addresses several of the topics identified in your subpoena:

- I am attaching a declaration Microsoft provided in *United States v. Bohannon*, No. CR 19-0039 (N.D. Cal.). It addresses, among other things, Microsoft's methods, policies, and procedures for identifying CSAM on its services, and reporting CSAM to NCMEC.

- The Microsoft Services Agreement ("MSA") is here, which incorporates the Microsoft Privacy Statement, here. These documents notify users of Microsoft policies relevant to CSAM issues. The page containing the Microsoft Privacy Statement links to a detailed change history, including for the period from July 30, 2018, to January 13, 2020.

- The Digital Safety Content Report addresses "[p]rotecting children online," here. This page addresses, among other things, Microsoft's procedures for identifying and reporting CSAM on its own services, and includes a FAQ section.

As to any topics in your subpoena that may not be addressed by this public information, we will talk with Microsoft about whether it will agree to conduct a reasonable search of its records. As I mentioned, for a few of the requests, I expect that Microsoft will object on grounds that the request is outside the bounds of its Rule 17 obligations.

If you are able to withdraw or narrow any of your requests following our conversation yesterday and the information above, please let me know, as that will expedite this process. We appreciate your extending the deadline for Microsoft's response to your subpoena while we work through these issues, and understand your interest in receiving a response to the subpoena by March 22. We also understand that you will confirm with your supervisor that you do not consider Microsoft to be under any sort of legal restraint to not speak with others about your subpoena.

We discussed setting a follow-up call for the end of this week. I will follow up with a proposed time once I speak with my client.

Best,
Megan

From: Gabriela Bischof <Gabriela_Bischof@fd.org>
Sent: Monday, March 6, 2023 4:10 PM
To: Crowley, Megan <MCrowley@cov.com>; Robert Ultan <Robert_Ultan@fd.org>
Cc: Goodwin, Chloe <CGoodwin@cov.com>; Karthik Raju <Karthik_Raju@fd.org>
Subject: Re: United States v. Burley, No. 21-CR-00198 EMC

[EXTERNAL]

From: Crowley, Megan <MCrowley@cov.com>
Sent: Monday, March 6, 2023 10:43:15 AM
To: Gabriela Bischof; Robert Ultan
Cc: Goodwin, Chloe; Karthik Raju
Subject: RE: United States v. Burley, No. 21-CR-00198 EMC

EXTERNAL SENDER
Thanks, Gabriela. I will give you a call at 1 pm PT.

From: Gabriela Bischof <Gabriela_Bischof@fd.org>
Sent: Monday, March 6, 2023 2:12 AM
To: Crowley, Megan <MCrowley@cov.com>; Robert Ultan <Robert_Ultan@fd.org>
Cc: Goodwin, Chloe <CGoodwin@cov.com>; Karthik Raju <Karthik_Raju@fd.org>
Subject: Re: United States v. Burley, No. 21-CR-00198 EMC

[EXTERNAL]
Hi Megan,

I'm free Monday after 10:30 PT, so just let me know what works for you. I'm happy to discuss an extension. Thanks for bringing the typo to our attention; the correct CyberTip Report number is 52016239. I can be reached at [redacted].

Thanks,
Gabriela

From: Crowley, Megan <MCrowley@cov.com>
Sent: Friday, March 3, 2023 2:52:31 PM
To: Robert Ultan
Cc: Goodwin, Chloe; Gabriela Bischof; Karthik Raju
Subject: RE: United States v. Burley, No. 21-CR-00198 EMC

EXTERNAL SENDER

Hi Rob, Gabriela and Karthik,

I'm sorry we haven't had a chance to speak. Is there a time on Monday when I could give you a call to discuss this subpoena? In the meantime, we would appreciate an extension of the subpoena response deadline (currently set for Monday, March 6) to allow for time to discuss the subpoena and gather responsive materials. Also, could you confirm that the Cybertip number listed in the subpoena is correct (56016239)?

Best,
Megan

From: Robert Ultan <Robert_Ultan@fd.org>
Sent: Thursday, March 2, 2023 4:03 PM
To: Crowley, Megan <MCrowley@cov.com>
Cc: Goodwin, Chloe <CGoodwin@cov.com>; Gabriela Bischof <Gabriela_Bischof@fd.org>; Karthik Raju <Karthik_Raju@fd.org>
Subject: RE: United States v. Burley, No. 21-CR-00198 EMC

[EXTERNAL]
Megan,

Thank you for your message. I am copying in the two attorneys I am working with on Mr. Burley's case, Assistant Federal Public Defenders Gabriela Bischof and Karthik Raju. One of them will contact you soon to discuss any questions you have about our subpoena and compliance with it.

Thanks,

Rob

Robert M. Ultan
Investigator
Office of the Federal Public Defender
450 Golden Gate Avenue #36106
San Francisco, CA 94102
[redacted]
415-436-7700 (main office)
415-436-7706 (fax)
robert_ultan@fd.org

From: Crowley, Megan <MCrowley@cov.com>
Sent: Thursday, March 2, 2023 12:54 PM
To: Robert Ultan <Robert_Ultan@fd.org>
Cc: Goodwin, Chloe <CGoodwin@cov.com>
Subject: United States v. Burley, No. 21-CR-00198 EMC

EXTERNAL SENDER

Dear Mr. Ultan,

We represent Microsoft in connection with your subpoena in the above-captioned matter. I would appreciate the chance to discuss the subpoena with you at your convenience.
Please let me know when you have a minute to discuss.

Thanks,
Megan

Megan A. Crowley
Pronouns: She/Her/Hers

Covington & Burling LLP
One CityCenter, 850 Tenth Street, NW
Washington, DC 20001-4956
T +1 202 662 5112 | mcrowley@cov.com
www.cov.com

COVINGTON